

CLAIMS

What is claimed is:

- 1 1. A method for managing access to messages in a network, the method comprising
2 the computer-implemented steps of:
3 receiving, from a first node in the network, a request for both a message identifier
4 that uniquely identifies the message and a key that may be used to encode
5 the message;
6 generating, in response to receiving the request, both the message identifier and the
7 key;
8 providing both the message identifier and the key to the first node to allow the
9 message to be encoded with the key to generate an encoded message;
10 receiving, from a second node in the network, a request for the key;
11 providing the key to the second node to allow the encoded message to be decoded
12 and the message to be retrieved using the key; and
13 managing access to the key based upon key policy criteria.
- 1 2. A method as recited in Claim 1, wherein managing access to the key based upon
2 key policy criteria includes deleting the key based upon the key policy criteria.
- 1 3. A method as recited in Claim 1, wherein managing access to the key based upon
2 key policy criteria includes only providing the key to authorized entities in
3 accordance with the key policy criteria.
- 1 4. A method as recited in Claim 1, wherein the steps are performed at a third node in
2 the network that is different from the first and second node.
- 1 5. A method as recited in Claim 4, wherein the steps are performed by a key server
2 executing at the third node.

- 1 6. A method as recited in Claim 1, further comprising verifying whether the first node
2 is authorized to obtain the key.
- 1 7. A method as recited in Claim 1, wherein the request from the second node for the
2 key specifies the message identifier, and the method further comprises verifying
3 that the second node is authorized to receive the key.
- 1 8. A method as recited in Claim 1, further comprising generating and storing data that
2 indicates that the key was provided to the first node or the second node.
- 1 9. A method as recited in Claim 1, further comprising generating and storing data that
2 indicates that the encoded message was decoded at the second node using the key.
- 1 10. A method as recited in Claim 6, further comprising generating and storing data that
2 indicates that the retrieved message was stored.
- 1 11. A method as recited in Claim 1, wherein the key policy criteria are managed at a
2 third node in the network that is different than the first and second nodes.
- 1 12. A method as recited in Claim 1, wherein the key policy criteria include one or more
2 of expiration date criteria, subject matter criteria and node identification criteria.
- 1 13. A method as recited in Claim 1, wherein the key policy criteria are dynamically
2 changed over time.
- 1 14. A method as recited in Claim 1, further comprising generating meta data that
2 specifies an attribute of the message, and wherein the step of deleting the key

3 based upon key policy criteria includes deleting the key by applying the key policy
4 criteria to the meta data.

1 15. A method as recited in Claim 1, further comprising after the key is deleted and the
2 next time the second node communicates with the network, instructing the second
3 node to delete the message retrieved from the encoded message using the key.

1 16. A method as recited in Claim 1, further comprising providing location data to the
2 second node that uniquely identifies a location where the key is maintained.
3

1 17. A method as recited in Claim 1, further comprising:
2 receiving and storing one or more encoded messages at the second node,
3 requesting, receiving, and storing at the second node, one or more keys, wherein
4 each of the keys is associated with one of the encoded messages that are
5 stored at the second node,
6 decoupling the second node from the network, and
7 decoding the encoded messages based on the keys.
8

1 18. A method as recited in Claim 1, further comprising:
2 generating a digital signature of the message and storing the digital signature in
3 association with the message, and
4 providing the digital signature to the second node to enable the second node to
5 validate the message.

1 19. A method as recited in Claim 1, further comprising:
2 receiving a request for a second message identifier and a second key,
3 encoding the encoded message using the second key to generate a twice-encoded
4 message, and

5 communicating the twice-encoded message to a third node in the network.

1 20. A method as recited in Claim 19, wherein
2 the message identifier is included in the encoded message, and
3 the method further comprises
4 extracting the message identifier from the encoded message prior to
5 encoding the encoded message using the second key, and
6 appending both the first message identifier and the second message
7 identifier to the twice-encoded message prior to communicating the
8 twice-encoded message to the third node.

1 21. A method as recited in Claim 1, further comprising:
2 extracting a second message identifier from a twice-encoded message,
3 receiving a request for a second key for the twice-encoded message,
4 providing the second key for the twice-encoded message,
5 decoding the twice-encoded message using the second key to recover the encoded
6 message,
7 extracting the first message identifier from the encoded message,
8 receiving a request for the first key to decode the encoded message,
9 providing the first key to allow decoding of the encoded message, and
10 decoding the encoded message using the first key to recover the message.

1 22. A method as recited in Claim 1, further comprising:
2 extracting a first message identifier and a second message identifier from a twice-
3 encoded message,
4 receiving a request for the first key and a second key for the twice-encoded
5 message,
6 providing the first key and the second key to allow decoding of the twice-encoded
7 message,

8 decoding the twice-encoded message using the second key to recover the encoded
9 message, and
10 decoding the encoded message using the first key to recover the message.

1 23. A computer-readable medium for managing access to messages in a network, the
2 computer-readable medium carrying one or more sequences of one or more
3 instructions which, when executed by one or more processors, cause the one or
4 more processors to perform the steps of:
5 receiving, from a first node in the network, both a request for a message identifier
6 that uniquely identifies the message and a key that may be used to encode
7 the message;
8 generating, in response to receiving the request, both the message identifier and the
9 key;
10 providing both the message identifier and the key to the first node to allow the
11 message to be encoded with the key to generate an encoded message;
12 receiving, from a second node in the network, a request for the key;
13 providing the key to the second node to allow the encoded message to be decoded
14 and the message to be retrieved using the key; and
15 managing access to the key based upon key policy criteria.

1 24. A computer-readable medium as recited in Claim 23, wherein managing access to
2 the key based upon key policy criteria includes deleting the key based upon the key
3 policy criteria.

1 25. A computer-readable medium as recited in Claim 23, wherein managing access to
2 the key based upon key policy criteria includes only providing the key to
3 authorized entities in accordance with the key policy criteria.

- 1 26. A computer-readable medium as recited in Claim 23, wherein the steps are
2 performed at a third node in the network that is different from the first and second
3 node.
- 1 27. A computer-readable medium as recited in Claim 26, wherein the steps are
2 performed by a key server executing at the third node.
- 1 28. A computer-readable medium as recited in Claim 23, further comprising one or
2 more additional instructions which, when executed by the one or more processors,
3 cause the one or more processors to perform the step of verifying whether the first
4 node is authorized to obtain the key.
- 1 29. A computer-readable medium as recited in Claim 23, wherein:
2 the request from the second node for the key specifies the message identifier, and
3 the computer-readable medium further comprises one or more additional
4 instructions which, when executed by the one or more processors, cause the
5 one or more processors to perform the step of verifying that the second
6 node is authorized to receive the key.
- 1 30. A computer-readable medium as recited in Claim 23, further comprising one or
2 more additional instructions which, when executed by the one or more processors,
3 cause the one or more processors to perform the step of generating and storing data
4 that indicates that the key was provided to the first node or the second node.
- 1 31. A computer-readable medium as recited in Claim 23, further comprising one or
2 more additional instructions which, when executed by the one or more processors,
3 cause the one or more processors to perform the step of generating and storing data
4 that indicates that the encoded message was decoded at the second node using the
5 key.

1 32. A computer-readable medium as recited in Claim 28, further comprising one or
2 more additional instructions which, when executed by the one or more processors,
3 cause the one or more processors to perform the step of generating and storing data
4 that indicates that the retrieved message was stored.

1 33. A computer-readable medium as recited in Claim 23, wherein the key policy
2 criteria are managed at a third node in the network that is different than the first
3 and second nodes.

1 34. A computer-readable medium as recited in Claim 23, wherein the key policy
2 criteria include one or more of expiration date criteria, subject matter criteria and
3 node identification criteria.

1 35. A computer-readable medium as recited in Claim 23, wherein the key policy
2 criteria are dynamically changed over time.

1 36. A computer-readable medium as recited in Claim 23, further comprising one or
2 more additional instructions which, when executed by the one or more processors,
3 cause the one or more processors to perform the step of generating meta data that
4 specifies an attribute of the message, and wherein the step of deleting the key
5 based upon key policy criteria includes deleting the key by applying the key policy
6 criteria to the meta data.

1 37. A computer-readable medium as recited in Claim 23, further comprising one or
2 more additional instructions which, when executed by the one or more processors,
3 cause the one or more processors to perform the step of after the key is deleted and
4 the next time the second node communicates with the network, instructing the
5 second node to delete the message retrieved from the encoded message using the
6 key.

1 38. A computer-readable medium as recited in Claim 23, further comprising one or
2 more additional instructions which, when executed by the one or more processors,
3 cause the one or more processors to perform the step of providing location data to
4 the second node that uniquely identifies a location where the key is maintained.
5

1 39. A computer-readable medium as recited in Claim 23, further comprising one or
2 more additional instructions which, when executed by the one or more processors,
3 cause the one or more processors to perform the steps of:
4 receiving and storing one or more encoded messages at the second node,
5 requesting, receiving, and storing at the second node, one or more keys, wherein
6 each of the keys is associated with one of the encoded messages that are
7 stored at the second node,
8 decoupling the second node from the network, and
9 decoding the encoded messages based on the keys.
10

1 40. A computer-readable medium as recited in Claim 23, further comprising one or
2 more additional instructions which, when executed by the one or more processors,
3 cause the one or more processors to perform the steps of:
4 generating a digital signature of the message and storing the digital signature in
5 association with the message, and
6 providing the digital signature to the second node to enable the second node to
7 validate the message.

1 41. A computer-readable medium as recited in Claim 23, further comprising:
2 receiving a request for a second message identifier and a second key,
3 encoding the encoded message using the second key to generate a twice-encoded
4 message, and

5 communicating the twice-encoded message to a third node in the network.

1 42. A computer-readable medium as recited in Claim 41, wherein
2 the message identifier is included in the encoded message, and
3 the method further comprises
4 extracting the message identifier from the encoded message prior to
5 encoding the encoded message using the second key, and
6 appending both the first message identifier and the second message
7 identifier to the twice-encoded message prior to communicating the
8 twice-encoded message to the third node.

1 43. A computer-readable medium as recited in Claim 23, further comprising:
2 extracting a second message identifier from a twice-encoded message,
3 receiving a request for a second key for the twice-encoded message,
4 providing the second key for the twice-encoded message,
5 decoding the twice-encoded message using the second key to recover the encoded
6 message,
7 extracting the first message identifier from the encoded message,
8 receiving a request for the first key to decode the encoded message,
9 providing the first key to allow decoding of the encoded message, and
10 decoding the encoded message using the first key to recover the message.

1 44. A computer-readable medium as recited in Claim 23, further comprising:
2 extracting a first message identifier and a second message identifier from a twice-
3 encoded message,
4 receiving a request for the first key and a second key for the twice-encoded
5 message,
6 providing the first key and the second key to allow decoding of the twice-encoded
7 message,

8 decoding the twice-encoded message using the second key to recover the encoded
9 message, and
10 decoding the encoded message using the first key to recover the message.

1 45. An apparatus for managing access to messages in a network, the apparatus
2 comprising a memory carrying one or more sequences of one or more instructions
3 which, when executed by one or more processors, cause the one or more
4 processors to perform the steps of:
5 receiving, from a first node in the network, both a request for a message identifier
6 that uniquely identifies the message and a key that may be used to encode
7 the message;
8 generating, in response to receiving the request, both the message identifier and the
9 key;
10 providing both the message identifier and the key to the first node to allow the
11 message to be encoded with the key to generate an encoded message;
12 receiving, from a second node in the network, a request for the key;
13 providing the key to the second node to allow the encoded message to be decoded
14 and the message to be retrieved using the key; and
15 managing access to the key based upon key policy criteria.

1 46. An apparatus as recited in Claim 45, wherein managing access to the key based
2 upon key policy criteria includes deleting the key based upon the key policy
3 criteria.

1 47. An apparatus as recited in Claim 45, wherein managing access to the key based
2 upon key policy criteria includes only providing the key to authorized entities in
3 accordance with the key policy criteria.

1 48. An apparatus as recited in Claim 45, wherein the steps are performed at a third
2 node in the network that is different from the first and second node.

- 1 49. An apparatus as recited in Claim 48, wherein the steps are performed by a key
2 server executing at the third node.
- 1 50. An apparatus as recited in Claim 45, wherein the memory further comprises one or
2 more additional instructions which, when executed by the one or more processors,
3 cause the one or more processors to perform the step of verifying whether the first
4 node is authorized to obtain the key.
- 1 51. An apparatus as recited in Claim 45, wherein:
2 the request from the second node for the key specifies the message identifier, and
3 the memory further comprises one or more additional instructions which, when
4 executed by the one or more processors, cause the one or more processors
5 to perform the step of verifying that the second node is authorized to
6 receive the key.
- 1 52. An apparatus as recited in Claim 45, wherein the memory further comprises one or
2 more additional instructions which, when executed by the one or more processors,
3 cause the one or more processors to perform the step of generating and storing data
4 that indicates that the key was provided to the first node or the second node.
- 1 53. An apparatus as recited in Claim 45, wherein the memory further comprises one or
2 more additional instructions which, when executed by the one or more processors,
3 cause the one or more processors to perform the step of generating and storing data
4 that indicates that the encoded message was decoded at the second node using the
5 key.
- 1 54. An apparatus as recited in Claim 50, wherein the memory further comprises one or
2 more additional instructions which, when executed by the one or more processors,

3 cause the one or more processors to perform the step of generating and storing data
4 that indicates that the retrieved message was stored.

1 55. An apparatus as recited in Claim 45, wherein the key policy criteria are managed at
2 a third node in the network that is different than the first and second nodes.

1 56. An apparatus as recited in Claim 45, wherein the key policy criteria include one or
2 more of expiration date criteria, subject matter criteria and node identification
3 criteria.

1 57. An apparatus as recited in Claim 45, wherein the key policy criteria are
2 dynamically changed over time.

1 58. An apparatus as recited in Claim 45, wherein the memory further comprises one or
2 more additional instructions which, when executed by the one or more processors,
3 cause the one or more processors to perform the step of generating meta data that
4 specifies an attribute of the message, and wherein the step of deleting the key
5 based upon key policy criteria includes deleting the key by applying the key policy
6 criteria to the meta data.

1 59. An apparatus as recited in Claim 45, wherein the memory further comprises one or
2 more additional instructions which, when executed by the one or more processors,
3 cause the one or more processors to perform the step of after the key is deleted and
4 the next time the second node communicates with the network, instructing the
5 second node to delete the message retrieved from the encoded message using the
6 key.

1 60. An apparatus as recited in Claim 45, wherein the memory further comprises one or
2 more additional instructions which, when executed by the one or more processors,

3 cause the one or more processors to perform the step of providing location data to
4 the second node that uniquely identifies a location where the key is maintained.
5

1 61. An apparatus as recited in Claim 45, wherein the memory further comprises one or
2 more additional instructions which, when executed by the one or more processors,
3 cause the one or more processors to perform the steps of:
4 receiving and storing one or more encoded messages at the second node,
5 requesting, receiving, and storing at the second node, one or more keys, wherein
6 each of the keys is associated with one of the encoded messages that are
7 stored at the second node,
8 decoupling the second node from the network, and
9 decoding the encoded messages based on the keys.
10

1 62. An apparatus as recited in Claim 45, wherein the memory further comprises one or
2 more additional instructions which, when executed by the one or more processors,
3 cause the one or more processors to perform the steps of:
4 generating a digital signature of the message and storing the digital signature in
5 association with the message, and
6 providing the digital signature to the second node to enable the second node to
7 validate the message.

1 63. An apparatus as recited in Claim 45, further comprising:
2 receiving a request for a second message identifier and a second key,
3 encoding the encoded message using the second key to generate a twice-encoded
4 message, and
5 communicating the twice-encoded message to a third node in the network.

1 64. An apparatus as recited in Claim 63, wherein

2 the message identifier is included in the encoded message, and
3 the method further comprises
4 extracting the message identifier from the encoded message prior to
5 encoding the encoded message using the second key, and
6 appending both the first message identifier and the second message
7 identifier to the twice-encoded message prior to communicating the
8 twice-encoded message to the third node.

1 65. An apparatus as recited in Claim 45, further comprising:
2 extracting a second message identifier from a twice-encoded message,
3 receiving a request for a second key for the twice-encoded message,
4 providing the second key for the twice-encoded message,
5 decoding the twice-encoded message using the second key to recover the encoded
6 message,
7 extracting the first message identifier from the encoded message,
8 receiving a request for the first key to decode the encoded message,
9 providing the first key to allow decoding of the encoded message, and
10 decoding the encoded message using the first key to recover the message.

1 66. An apparatus as recited in Claim 45, further comprising:
2 extracting a first message identifier and a second message identifier from a twice-
3 encoded message,
4 receiving a request for the first key and a second key for the twice-encoded
5 message,
6 providing the first key and the second key to allow decoding of the twice-encoded
7 message,
8 decoding the twice-encoded message using the second key to recover the encoded
9 message, and
10 decoding the encoded message using the first key to recover the message.